INFORMATION SECURITY POLICY COMPLIANCE IN SMEs

Dávid Sklenár[a] **– Kristína Čimová**[b]

[a] Faculty of Economics, Paneuropean University, Tematinska 10, Bratislava, Slovak Republic,
e-mail: davids@iktcom.sk
[b] School of Social and Political Sciences, University of Glasgow, Glasgow, UK,
e-mail: k.cimova.1@research.gla.ac.uk

Abstract: In the paper we examined attitudes, intent and adherence to information security policies and procedures in SMEs in Slovakia. Data were collected from the employees of several SME in Slovak republic. Not all enterprises have established information security policies and procedures. Only 443 respondents (from 722) worked in a SME that had formulated an information security policy. The impact of the size of enterprises, age on the measured variables has not been shown. IT related jobs, managerial post and education level of the respondents has shown significant impact in the evaluation of attitudes, intentions and adherence to information security policies and procedures. From statistical methods we use the maximum-likelihood estimation of the polychoric correlation coefficient. The calculations have been carried out in R statistical programming environment[1].
Key words: information security policies, SME, Slovak republic, polychoric correlation coefficient
JEL: D89, O15

Introduction

Information security (IS) is defined as the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability. An information security policy is a set of policies, regulations, rules and procedures that govern how an organization manages, protects and distributes information. Compliance with an information security policy is defined as the action that users take to ensure the protection of information security.

Information security awareness can be defined as an individual's passive involvement and increased interest in information security issues. NAMJOO, C. ET AL.[2] (2008) concluded by their research that awareness of information security is about ensuring that all employees are aware of the rules and regulations relating to the security of information in the enterprise.

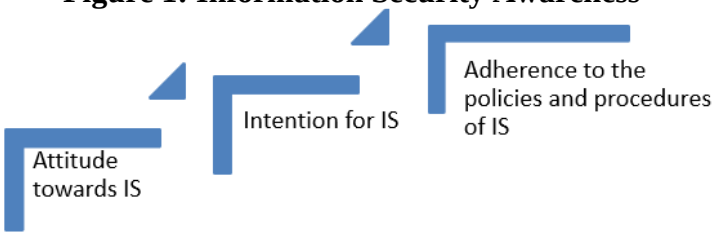
It is important that people not only have the necessary knowledge of information security, but also have a positive relationship to it. We have also noted that culture can guide how employees think, act and feel, thereby affecting the organization's activities and the effectiveness of information protection.

[1] The authors are a PhD. Students.
[2] NAMJOO, C. – DAN, K. – JAHYUN, G. – ANDY, W. (2008): Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action.

A study by WALY, N., TASSABEHJI, R. and KAMALA, M.[3] (2012) contributes to knowing what factors influence employee behaviour towards adherence to the organization's information security policy. The categories of factors identified are differently monitored by employees working in the health, trade and education sectors. PALISZKIEWICZ, J.[4] (2019) also addressed the identification of success factors for information security policies. KHAN, B.[5] et al. (2011) developed a five-step model for measuring information security awareness. We use modified three step ladder model for measuring information security awareness.

A number of researches have been conducted to understand the factors that influence employees' intent and decision to adhere to information security policy. As several authors have found (BULGURCU, B.[6] et al. (2009), BULGURCU, B. et al[7]. (2010), AL-OMARI, A.[8] et al., (2012), HUMAIDI, N. and BALAKRISHNAN, V.[9] (2015)) awareness of information security policy has a positive impact on its compliance. HU, Q., DINEV, T., HART, P. and COOKE, D.[10] (2012) argue that the involvement of top management in information security management has a significant positive impact on both attitude and staff behaviour in adherence to information security policies.

Figure 1: Information Security Awareness



Source: Author's own processing according to KHAN, B. et al. (2011)

Despite research in other scientific areas that suggest that demographic factors play an important role in influencing behaviour, there are few articles to examine the impact of demographic characteristics of employees (age, gender, education) on adherence to information security policies, MOODY, G.D., SIPONEN, M. and PAHNILA, S.[11] (2018), CHUA, H. N. et al.[12] (2018) on the basis of research on a sample of 607 respondents have shown that age, ethnicity, industry and level of education have a significant impact on

[3] WALY, N. – TASSABEHJI, R. – KAMALA, M. (2012): Improving organisational information security management: The impact of training and awareness. pp. 1270-1275
[4] PALISZKIEWICZ, J. (2019): Information Security Policy Compliance: Leadership and Trust.
[5] KHAN, B. – ALGHATHBAR, K. S. – NABI, S. I, –KHAN, M. K. (2011): Effectiveness of information security awareness methods based on psychological theories.
[6] BULGURCU, B. – CAVUSOGLU, H. – BENBASAT, I. (2009): Roles of information security awareness and perceived fairness in information security policy compliance.
[7] BULGURCU, B. – CAVUSOGLU, H. – BENBASAT, I. (2010): Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness.
[8] AL-OMARI, A. –, EL-GAYAR, O. – DEOKAR, A. (2012): Information security policy compliance: the role of information security awareness.
[9] HUMAIDI, N. – BALAKRISHNAN, V. (2015): Leadership styles and information security compliance behaviour: the mediator effect of information security awareness.
[10] HU, Q. – DINEV, T. – HART, P. – COOKE, D. (2012): Managing employee compliance with information security policies: The critical role of top management and organizational culture.
[11] MOODY, G.D. – SIPONEN, M. – PAHNILA, S. (2018): Toward a unified model of information security policy compliance.
[12] CHUA, H. N. – WONG, S. F. – LOW, Y. C. – CHANG, Y. (2018): Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations.

information security awareness and compliance. They found that those with a higher awareness of information security policy tended to achieve a higher level of compliance. CHUA, H. N. et al[11]. (2018) concluded by their research that there is a strong correlation between awareness and compliance with data protection policy. The authors themselves state that this result contradicts the findings of ALBRECHTSEN, E.[13] (2007). The authors explain the reasons for these differences by cultural differences, since ALBRECHTSEN, E.[12] (2007) conducted his study in Germany, while the research sample CHUA, H. N. et al.[11] (2018) was from Malaysia. This argument is acceptable in light of the findings of DINEV, T., GOO, J. and HU, Q.[14] (2009), who on a sample of respondents from South Korea and the US have shown that cultural factors are statistically significant in influencing the behavior of IT users.

Human factors play an important role in computer security. It is widely accepted that employees of an organization are often a weak link in protecting their information assets. In the paper with METALIDOU, E. et al.[15] (2014) focus on the impact of the human factor in information security. Insufficient IT skills of employees pose a risk of unintentional damage to the company's information assets. Information security awareness is considered by METALIDOU, E. et al.[14] (2014) as the main tool in overcoming these shortcomings.

Many organizations recognize that their employees, who are often seen as the weakest link in information security, can also be of great benefit in efforts to reduce the risk of information security. As employees who adhere to the organization's information security rules and regulations are key to enhancing information security, understanding compliance is key to organizations wishing to use their human capital, according to BULGURCU, B., CAVUSOGLU, H. and BENBASAT, I.[16] (2010).

Much of the research into the security of information systems focused on employee behavior is focused on compliance, resp. non-compliance and misuse of resources (WARKENTIN, M. and WILLISON, R.[17] 2009). The theory of discouragement is one of the most widely used theories in security research of information systems security. ISO / IEC 27002, one of the most widespread standards for information security management, also draws on deterrence theory - from policy recommendations, guidelines and awareness programs that clearly define the consequences and sanctions for employees who misuse company resources. The standard also prescribes monitoring of the access system and control mechanisms based on the assumption that increased detection security discourages security breaches.

People make their decisions about committing or refraining from crime by maximizing their benefits and minimizing costs. The classic deterrence theory focuses on formal (legal) sanctions and assumes that the greater the perceived certainty, severity and integrity (speed) of sanctions for an illegal act, the more individuals are discouraged. Extensions of the classic deterrent model include informal sanctions such as social disapproval, shame. Current deterrence theory assumes that individuals include the perceived risks and costs of both formal and informal sanctions when deciding whether or not to engage

[13] ALBRECHTSEN, E. (2007): A qualitative study of users' view on information security.
[14] DINEV, T. – GOO, J. – HU, Q. (2009): User behavior towards protective information technologies: the role of national cultural differences.
[15] METALIDOU, E. et al. (2014): The human factor of information security: Unintentional damage perspective.
[16] BULGURCU, B. – CAVUSOGLU, H. – BENBASAT, I. (2009): Roles of information security awareness and perceived fairness in information security policy compliance.
[17] WARKENTIN, M. – WILLISON, R. (2009): Behavioural and policy issues in information systems security: the insider threat.

in illegal activity, according to D'ARCY, J. and HERATH, T.[18] (2011). Empirical results associate low self-control with many criminal and deviant activities. By JACOBS, B.A.[19] (2010) The theoretical argument is that individuals with low self-control are more susceptible to illegal activities in an impulsive manner and therefore less responsive to the threat of punishment.

Efforts to raise security awareness and monitor computers have had less impact on the intent of misusing information systems for people with a high level of confidence in their ability to use computers, found D'ARCY, J. and HOVAV, A.[20] (2009). The reason is that good knowledge in this regard leads some individuals to believe that they can circumvent security measures and get out of their breach with a low threat of punishment.

The aim of the paper is information security policy compliance in SMEs. Based on the above mentioned knowledge from literature, we will ask in the identification part of the questionare in our empirical research about gender, age, education, position of respondent in employment, level of IT skills. We will also ask the respondents about the size of the company in which they work. We will also use a three stage model to measure awareness of information security . Respondents will be asked about their knowledge, attitudes and intentions in adhering to information security policies and real adherence of these.

We utilised the methods of scientific description and abstraction, comparison, analysis and synthesis, as well as inductive and deductive techniques in this article. From statistical methods we use the maximum-likelihood estimation of the polychoric correlation coefficient described by OLSSON, U.[21] (1979). The calculations have been carried out in R statistical programming environment (R Core Team, 2018[22]).

1 Methodology

Ordinal variables, also called ordered category variables, are variables whose values are ordered, but cannot be added or multiplied. When a variable's categories have a natural order, researchers speak on an ordinal variable. All indicators in our research are ordinal or dichotomous. The probability distribution of the ordinal responses are not normal, in particular if very low or high values are frequently chosen.

Independence of two ordinal variables can be tested with a number of tests, e.g., the Pearson chi-square test for contingency tables. If random variables $X$and Y are statistically dependent, then it is often of interest to estimate some measure of association. According to EKSTROM, J. [23] (2008) the polychoric correlation coefficient is one such measures of association, especially defined for ordinal variables. UEBERSAX, J.S.[24] (2015) uses the term 'latent continuous correlations' both for tetrachoric and polychoric correlations. Similarly to Pearson's correlation coefficient, the polychoric correlation coefficient acquires values from the interval $\langle -1, 1\rangle$. The values close to zero indicate independence. For a correct evaluation and interpretation of the polychoric coefficient values, we need to test its statistical significance.

[18] D'ARCY, J. – HERATH, T. (2011): A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.
[19] JACOBS, B. A. (2010): Deterrence and deterrability.
[20] D'ARCY, J. – HOVAV, A. (2009): Does one size fit all? examining the differential effects of IS security countermeasures.
[21] OLSSON, U. (1979): Maximum likelihood estimation of the polychoric correlation coefficient.
[22] R Core Team (2018): R: A language and environment for statistical computing.
[23] EKSTROM, J. (2008): On the relation between the phi-coefficient and the tetrachoric correlation coefficient.
[24] UEBERSAX, J. S. (2015): Introduction to the Tetrachoric and Polychoric Correlation Coefficients.

This study uses explanatory research methodology to conduct the research, and the method of the research is a survey. Data were collected from the employees of several SME in Slovak republic. Not all of these enterprises have established information security policies and procedures. The survey participants answered through Google Drive (electronic questionnaire). The process of data collection was conducted from first May to end of September 2019. The questionnaire included 19 questions. In this paper we analyze the results of the responses related to information security awareness.

We test several scientific hypotheses in our case study. We assume that the larger the enterprise, the more likely it is to value its information, and therefore it is more likely that the enterprise will place greater emphasis on adherence to information security policies. From the literary sources mentioned in the introduction we know that age, gender or level of knowledge in the IT may have, but does not have to have, an impact on an individual's adherence to the policies of information security. Based on this we have formulated the following hypothesis.

- Hypothesis 1: The adherence to the policies of information security in SME is dependent on the size of the enterprises.
- Hypothesis 2 (a-d): The attitude towards and the intention behind the adherence to policies of information security in SME are both dependent on the following:
  a) the gender of the employee,
  b) the age of the employee,
  c) the position of employee within the business itself,
  d) the occupational focus of the employee (IT or other).

We examined attitudes, intent and adherence to information security policies and procedures in SMEs in Slovakia. The answers have lower score if the attitudes, intents and adherence to information security policies and procedures are all the better. The answers devised, available for the respondents to choose from are outlined below in Tables 1,2, and 3.

Table 1: The attitudes to information security policies and procedures

Score	*Answer*
1	Information security policies and procedures should be followed.
2	It is beneficial to follow information security policies and procedures. benefit
3	Adherence to information security policies and procedures reduces the risk of security breaches.
4	Compliance with information security policies and procedures is a good idea.
5	Adherence to information security policies and procedures is unnecessary.

Table 2: The intentions to information security policies and procedures

Score	*Answer*
1	I am sure that I will follow the information security policies and procedures.
2	I will continue to follow information security policies and procedures to protect information assets.
3	My intention is to follow information security policies and practices.
4	I will follow information security policies and procedures in my work whenever possible.
5	I do not intend to adhere to information security policies and procedures.

Table 3: The adherences to information security policies and procedures

Score	*Answer*
1	I wholeheartedly adhere to information security policies and procedures.
2	I adhere to information security policies and procedures.
3	I mostly adhere to information security policies and procedures.
4	I adhere to information security policies and procedures whenever possible.
5	I do not adhere to information security policies and procedures

2 Survey findings

722 respondents were involved in our survey. Only 443 respondents worked in a SME that had formulated an information security policy. There is no micro enterprise with an information security policy in our survey. The structure of respondents is described in Table 4.

Table 4: Respondents' characteristics

Measure	*Items*	*Percent*
Gender	Male	37,25
	Female	62,75
Size of enterprise	Small enterprise	44,70
	Medium-sized enterprise	55,30
Age group (years)	Up to 30	19,19
	31-40	28,67
	41-50	24,83
	51-60	17,16
	61+	10,16
Education	Primary	3,39
	Secondary	3,39
	Secondary with GCSE	62,98
	Tertiary	30,25
Position within enterprise	Managerial function	11,29
	Non-managerial function	88,71
Occupational focus	IT related	67,49
	Other	32,51

Source: Author's own data

Table 5 includes the values of the polychoric correlation coefficient, calculated through the maximum-likelihood method and its standard deviations. Table 6 contains the p-values of polychoric correlation coefficients.

Table 5: The polychoric correlation coefficient values and its *standard error*

Measure	*Polychoric correlation coefficient*		
	Attitude to IS policies and procedures	*Intention to IS policies and procedures*	*Adherence to IS policies and procedures*
Gender	0,01717 (0,0686)	-0,00545 (0,07233)	0,00838 (0,06422)

Measure	*Polychoric correlation coefficient*		
	Attitude to IS policies and procedures	*Intention to IS policies and procedures*	*Adherence to IS policies and procedures*
Size of enterprise	0,086 (0,06713)	0,1225 (0,07056)	0,06069 (0,06279)
Age	0,04395 (0,05592)	0,1048 (0,05856)	0,06581 (0,05196)
Education	-0,1724 (0,06183)	-0,2024 (0,06414)	-0,2344 (0,05658)
Managerial position	0,2535 (0,08385)	0,3733 (0,08684)	0,6371 (0,06008)
IT related job	-0,4006 (0,06358)	-0,6629 (0,0517)	-0,7226 (0,03518)
Attitude to IS policies and procedures	x	0,9189 (0,0167)	0,6037 (0,03902)
Intention to IS policies and procedures	0,9189 (0,0167)	x	0,8263 (0,0262)
Adherence to IS policies and procedures	0,6037 (0,03902)	0,8263 (0,0262)	x

Source: Author's own data

Table 6: p - values for polychoric correlation coefficients

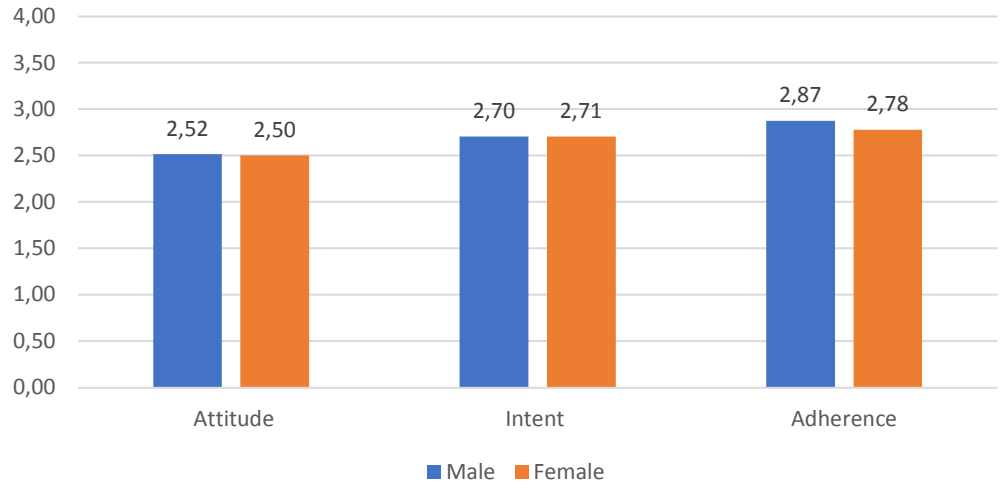
Measure	*Polychoric correlation coefficient*		
	Attitude to IS policies and procedures	*Intention to IS policies and procedures*	*Adherence to IS policies and procedures*
Gender	0,6936	0,2438	0,3036
Size of enterprise	0,3926	0,1251	0,6801
Age	0,5009	0,6834	0,0941
Education	1,92E-20	6,08E-14	3,32E-31
Managerial position	0,0196	0,4134	0,6975
IT related job	1,17E-04	2,08E-02	2,91E-11
Attitude to IS policies and procedures	x	3,76E-05	3,78E-07
Intention to IS policies and procedures	3,76E-05	x	7,43E-06
Adherence to IS policies and procedures	3,78E-07	7,43E-06	x

Source: Author's own data

With regards to gender there are barely noticeable differences of attitude, intent and adherence to information security policies and procedures. All p-values for polychoric correlation coefficients are greater than 0.05 (Table 6) The significance of gender on of

attitude, intent and adherence to information security policies and procedures has therefore not been shown in our case study.

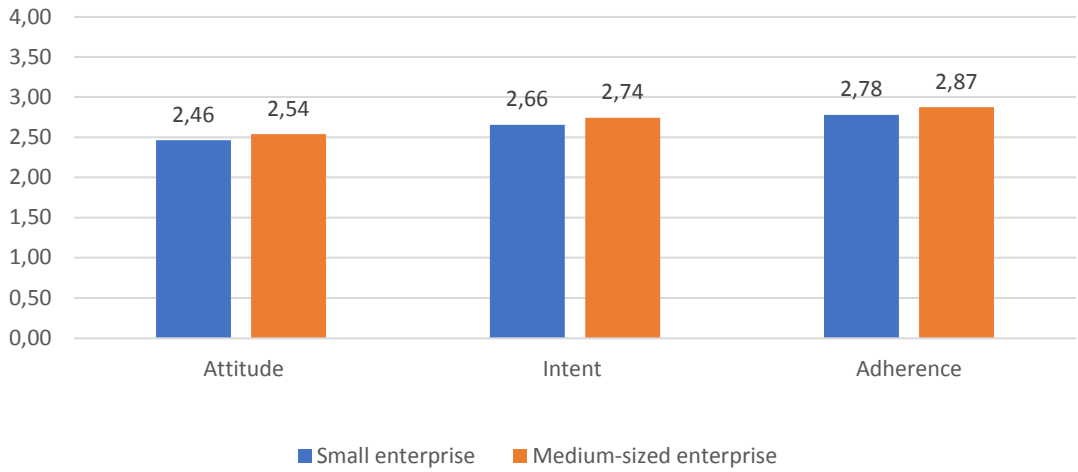
Figure 2: The evaluation of attitude, intent and adherence to information security policies and procedures with regards to gender



Source: Author's own data and graphics

With regards to enterprise size, the impact of this variable on the intentions, attitudes and adherence to policies and procedures of information security is also of little significance. The p-values for polychoric correlation coefficients are all markedly greater than 0.05 (Table 6). The impact of the size of enterprises on the measured variables has therefore not been shown in our case study.

Figure 3: The evaluation of attitude, intent and adherence to information security policies and procedures with regards to enterprise size

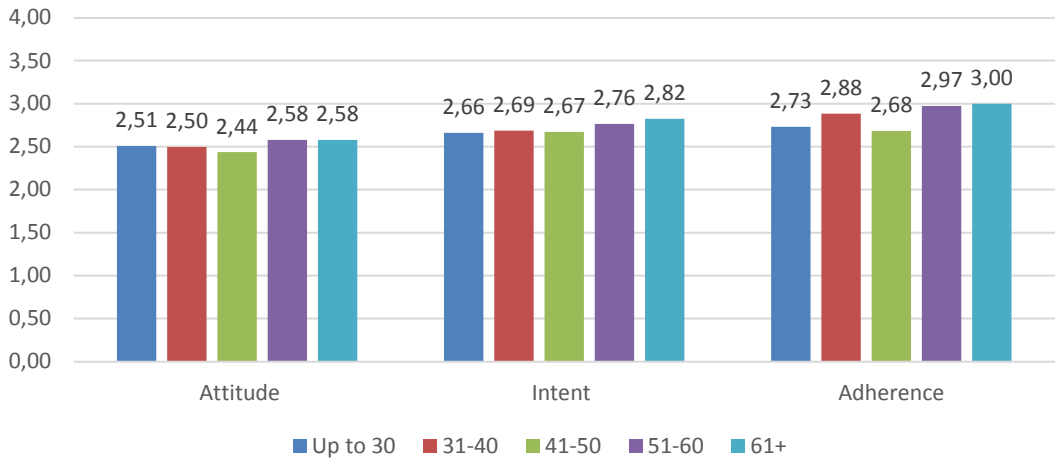


Source: Author's own data and graphics

There are not significant variation between evaluation of attitudes, intentions and adherence to information security policies and procedures for examined age groups. The p-values for polychoric correlation coefficients are greater than 0.05 (Table 6). In the case of adherence the p-value is 0.0941, which indicates significance on the level 0.10. Our case

study has therefore not shown statistical significance (on significance level 0,05) of the impact of age on the measured variables. The respondents in the age group of 41-50 behave more responsibly. The same goes for the youngest respondents of under 30 years old. The lack of attitude, intent and adherence to information security policies and procedures increases with age.

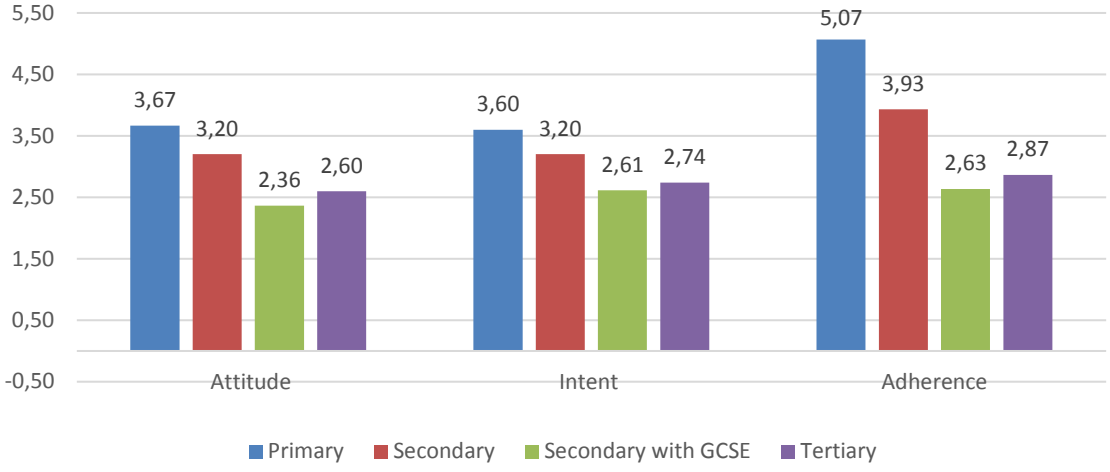
Figure 4: The evaluation of attitude, intent and adherence to information security policies and procedures focusing on age group



Source: Author's own data and graphics

With regards to education, there is definitely noticeable variation in terms of attitudes, intentions and adherence to policies and procedures targeting information security. All p - values of the polychoric correlation coefficients are smaller than 0.05 (Table 6). The coefficients are negative which is why we can conclude that with the increase of educational levels, the attitudes, intentions and adherence to policies and procedures of information security improve. The most responsible are respondents with a completed secondary education. A very irresponsible attitude is displayed by respondents with primary education. These respondents can present as a threat to their workplaces with regards to information security.

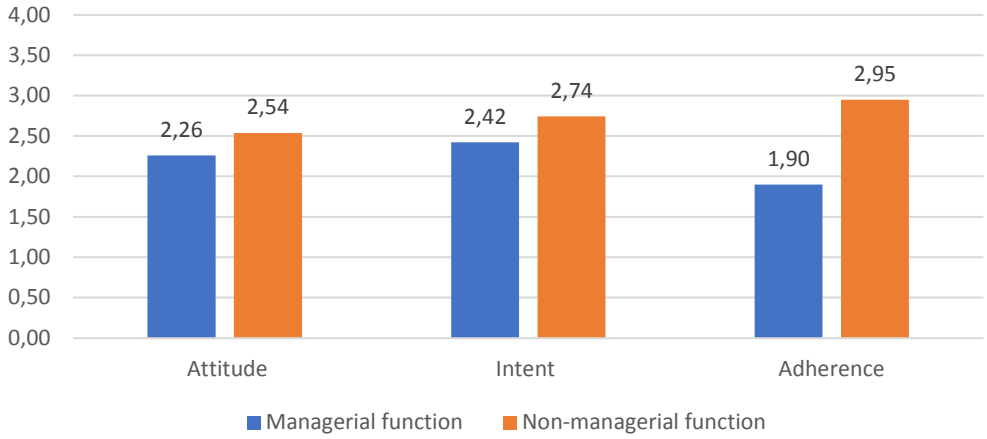
Figure 5: The evaluation of attitude, intent and adherence to information security



Source: Author's own data and graphics

Our case study confirms the results of the authors who conclude that those in managerial positions have a higher level of responsibility when approaching information security. It was not the goal of our study to explain why this is the case. In terms of significance the difference between those in managerial positions and the rest is on the level of 0.05 significance.

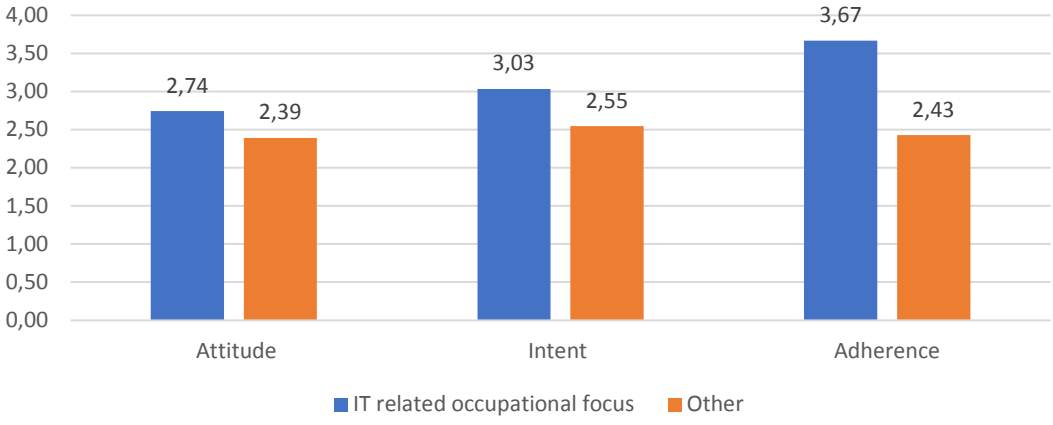
Figure 6: The evaluation of attitude, intent and adherence to information security policies and procedures focusing on position in company



Source: Author's own data and graphics

The occupational focus (IT or other) of the respondents has shown statistical significance in relation to our measured variables. The p-values of the polychoric correlation coefficient significance are all lower than 0.05 (Table 6). The most responsible are those respondents who work in a different area than IT. A possible reason for this can be too great a trust in one's own abilities in IT related jobs, or the conviction that the business will not be threatened. A possible solution could be relevant changes in the presentation and enforcement of information security policies in these businesses; as well as special educational programmes for IT employees.

Figure 7: The evaluation of attitude, intent and adherence to information security policies and procedures focusing on occupation



Source: Author's own data and graphics

The results of the case study confirm the assumed highly significant correlation between the attitude, intent and adherence to information security policies and procedures (Table6).

Conclusions

Some organisations agree that the employees who are often considered to be the weak link in information security policy enforcement can actually become the greatest asset in lowering the risks connected to information security. Since the employees who abide by the set out rules and regulations are the key to the strengthening of the information security processes, the understanding of their behaviour is key for organisations seeking to properly harness the human capital of the given enterprises.

Human factors often play a key role in IT security. Generally, the understanding is that employees of enterprises are often the weak links in protecting the information itself. Some of our results are in line with the findings of the cited authors. The results of our study confirmed some significant impact of the following on evaluation of attitude, intent and adherence to information security policies and procedures:

Impact of age on the adherence to policies and procedures has not shown a statistically significant correlation.

Education - With the increased level of education, awareness of and adherence to the policies set out to protect information increases. The most responsible are those with secondary education completed. The least responsible are those with primary education completed. These employees can pose a threat in terms of information security.

In case of managerial positions versus other positions, the difference between their attitudes to information security is significant.

Occupational focus - IT related jobs or other jobs of the respondents has shown significant impact in the evaluation of attitudes towards, intentions behind and adherence to policies and procedures within information security.

References:

1. ALBRECHTSEN, E. (2007): A qualitative study of users' view on information security. In: *Computers and security*, 2007. Vol. 26, No. 4, pp. 276-289. ISSN 0167-4048.
2. AL-OMARI, A. – EL-GAYAR, O. – DEOKAR, A. (2012): Information security policy compliance: the role of information security awareness. In: *AMCIS 2012 Proceedings*, Seattle, 2012, pp. 1-10
3. BULGURCU, B. – CAVUSOGLU, H. – BENBASAT, I. (2009): Roles of information security awareness and perceived fairness in information security policy compliance. In: *Proceedings of the Fifteenth Americas Conference on Information Systems, AMCIS 2009*, pp. 1-9
4. BULGURCU, B. – CAVUSOGLU, H. – BENBASAT, I. (2010): Information security policy compliance: an empirical study of rationality-based beliefs and information security awarenes. In: *MIS Quarterly Executive*, 2010. Vol. 34, pp. 523-548. ISSN 1540-1960.
5. D'ARCY, J. – HERATH, T. (2011): A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findingpp. In: *European Journal of Information Systems*, 2011. Vol. 20, No. 6, pp. 643-658. ISSN 0960-085X.
6. D'ARCY, J. – HOVAV, A. (2009): Does one size fit all? examining the differential effects of IS security counter measures. In: *Journal of Business Ethics*, 2009. Vol. 89, No. 1, pp. 59-71. ISSN 0167-4544.

7. DINEV, T. – GOO, J. – HU, Q. (2009): User behavior towards protective information technologies: the role of national cultural differences. In: *Information Systems Journal*, 2009. Vol. 19, pp. 391-412. ISSN 1365-2575.
8. DRAGULESCU, A. A. – ARENDT, C. (2018): xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.1. [Citované: 12. 10. 2019] Dostupné na internete: https://CRAN.R-project.org/package=xlsx
9. EKSTROM, J. (2008): On the relation between the phi-coefficient and the tetrachoric correlation coefficient. In *Contributions to the Theory of Measures of Association for Ordinal Variables*. Upsaliensipp: Acta Universitatis Upsaliensipp. [Citované: 12. 05. 2019] Dostupné na internete: http://www.diva-portal.org/smash/record.jsf?pid=diva 2%3A210881&dswid=-3931
10. FOX, J. (2019): polycor: Polychoric and Polyserial Correlationpp. R package version 0.7-10. [Citované: 12. 05.2019] Dostupné na internete: https://CRAN.R-project.org/ package=polycor
11. HU, Q. –DINEV, T. – HART, P. – COOKE, D. (2012): Managing employee compliance with information security policies: The critical role of top management and organizational culture. In: *Decision Sciences*, 2012. Vol. 43, No. 4, pp. 615-660. ISSN 1540-5915.
12. HUMAIDI, N. – BALAKRISHNAN, V. (2015): Leadership styles and information security compliance behavior: the mediator effect of information security awareness. In: *International Journal of Information and Education Technology,* 2015. Vol. 5, No. 4, pp. 311.318. ISSN 2010-3689.
13. CHUA, H. N. – WONG, PP. F. – LOW, Y. C. – CHANG, Y. (2018): Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizationss. In*: Telematics and Informatics*, 2018. Vol. 35, pp. 6, pp. 1770-1780. ISSN 0736-5853.
14. JACOBS, B. A. (2010): Deterrence and deterrability. In*: Criminology*, 2010. Vol. 48, No. 2, pp. 417-441. ISSN 1745-9125.
15. KHAN, B. – ALGHATHBAR, K. P. – NABI, P. I. – KHAN, M. K. (2011): Effectiveness of information security awareness methods based on psychological theoriess. In: *African Journal of Business Management*, 2011. Vol. 5, No. 26, pp. 862-868. ISSN 1993-8233.
16. METALIDOU, E. – MARINAGI, C. – TRIVELLAS, P. – EBERHAGEN, N. – SKOURLAS, C. – GIANNAKOPOULOS, G. (2014): The human factor of information security: Unintentional damage perspective. In: *Procedia-Social and Behavioral Sciences*, 2018. No. 147, pp. 424-428. ISSN 1877-0428.
17. MOODY, G.D. – SIPONEN, M. – PAHNILA, PP. (2018): Toward a unified model of information security policy compliance. In: *MIS Quarterly*, 2018. Vol. 42, No. 1, pp. 285-311. ISSN 2162-9730.
18. NAMJOO, C. –DAN, K. – JAHYUN, G. – ANDY, W. (2008): Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. In: *Information Management & Computer Security*, 2008. Vol. 16, No.5, pp. 484-501. ISSN 0968-5227.
19. OLSSON, U. (1979): Maximum likelihood estimation of the polychoric correlation coefficient. In: *Psychometrika.* No. 44, pp. 443-460.
20. PALISZKIEWICZ, J. (2019): Information Security Policy Compliance: Leadership and Trust. In: *Journal of Computer Information Systems*, 2019, pp. 1-7. ISSN 0887-4417.

21. R Core Team (2018): R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. [Citované: 12. 05. 2019] Dostupné na internete: https://www.R-project.org/
22. UEBERSAX, J. P. (2015): "Introduction to the Tetrachoric and Polychoric Correlation Coefficient. [Citované: 10. 02. 2019] Dostupné na internete: h*ttp://www. John-Uebersax.Com/Stat/Tetra.Htm*.
23. WALY, N. – TASSABEHJI, R. – KAMALA, M. (2012): Improving organisational information security management: The impact of training and awareness. In: *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems,* Liverpool, UK. 2012. pp. 1270-1275. ISBN 978-0-7695-4749-7.
24. WARKENTIN, M. – WILLISON, R. (2009): Behavioural and policy issues in information systems security: the insider threat. In: *European Journal of Information Systems,* 2009. Vol. 18, No. 2, pp. 101-105. ISSN 1476-9344.

Contacts:
Mgr. Dávid Sklenár
Faculty of Economics and Entrepreneurship
Pan-European University
Tematinska 10
851 05 Bratislava
Slovak Republic
e-mail: davids@iktcom.sk

Mgr. Kristína Čimová
School of Social and Political Sciences
University of Glasgow
Glasgow
United Kingdom
e-mail: k.cimova.1@research.gla.ac.uk